

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-288453  
(43)Date of publication of application : 04.10.2002

(51)Int.Cl.

G06F 17/60  
G06F 12/00  
G06F 12/14  
G06F 17/30  
H04Q 7/38  
H04L 9/08

(21)Application number : 2001-090489

(71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 27.03.2001

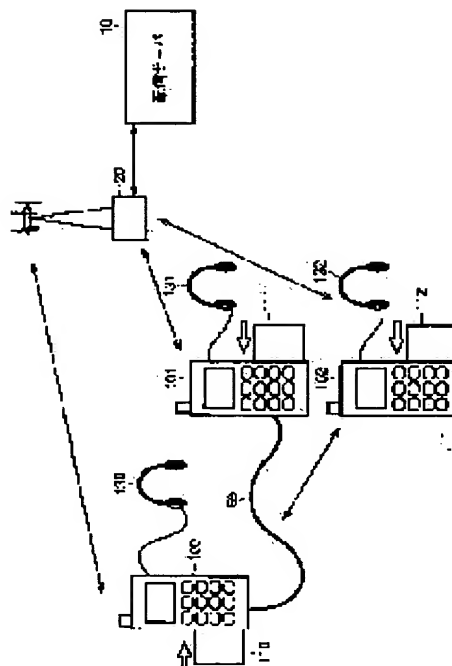
(72)Inventor : YASUDA CHOMEI

## (54) INFORMATION TERMINAL

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an information terminal which retrieves a storage place on of ciphered contents data, which a user wants to acquire, and acquires ciphered contents data from this retrieved storage place.

**SOLUTION:** When wanting to newly purchase music of an artist A, the user of a mobile phone 100 receives the retrieval result of the artist A from a delivery server 10. The mobile phone 100 retrieves a memory card, where ciphered contents data included in the retrieval result received from the delivery server 10 is stored, on the basis of a database. When ciphered contents data is stored in a memory card 111, the mobile phone 100 copies ciphered contents data from a mobile phone 101 and receives a license from the delivery server 10.



## LEGAL STATUS

[Date of request for examination] 05.08.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(11)特許出願公開番号

特開2002-288453

( P2002-288453A)

(43)公開日 平成14年10月4日(2002.10.4)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 17/60	3 0 2	G 0 6 F 17/60	3 0 2 E 5 B 0 1 7
	Z E C		Z E C 5 B 0 7 5
	1 4 2		1 4 2 5 B 0 8 2
	5 0 2		5 0 2 5 J 1 0 4
12/00	5 4 5	12/00	5 4 5 Z 5 K 0 6 7
審査請求 未請求 請求項の数 6 O L (全 26 頁) 最終頁に続く			

(21)出願番号 特願2001-90489(P2001-90489)

(22)出願日 平成13年3月27日(2001.3.27)

(71)出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72)発明者 安田 朝明

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

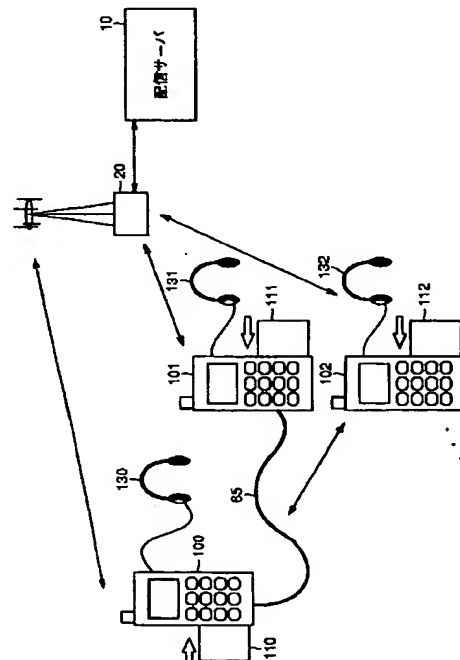
[最終頁に続く](#)

(54) 【発明の名称】 情報端末装置

(57) 【要約】

【課題】 ユーザが取得したい暗号化コンテンツデータの格納場所を検索し、その検索した格納場所から暗号化コンテンツデータを取得する情報端末装置を提供する。

【解決手段】 携帯電話機１００のユーザは、新たにアーティストＡの曲を購入したいとき、そのアーティストＡの検索結果を配信サーバ１０から受信する。携帯電話機１００は配信サーバ１０から受信した検索結果に含まれる暗号化コンテンツデータがどのメモリカードに格納されているかをデータベースに基づいて検索する。そして、携帯電話機１００は、暗号化コンテンツデータがメモリカード１１１に格納されているとき携帯電話機１０１から暗号化コンテンツデータをコピーし、ライセンスを配信サーバ１０から受信する。



## 【特許請求の範囲】

【請求項 1】 複数の情報端末装置において作成され、かつ、暗号化コンテンツデータを管理するための複数のデータベースを検索して前記暗号化コンテンツデータと前記暗号化コンテンツデータを再生するためのライセンスとを取得する情報端末装置であって、外部とのデータのやり取りを行なう送受信部と、指示を入力するためのキー操作部と、前記複数のデータベースと一覧表とを記憶する記憶部と、制御部とを備え、前記複数のデータベースの各々は、複数の暗号化コンテンツデータを特定するための複数のコンテンツ特定情報と、前記暗号化コンテンツデータに対応するライセンスの有無を示す複数のライセンス情報と、前記暗号化コンテンツデータおよび前記ライセンスが記録されたデータ記録装置を特定するための複数の記録装置特定情報とを含み、前記一覧表は、前記複数のデータベースを特定するための複数のデータベース特定情報と、前記複数のデータベースの各々が生成された情報端末装置を特定するための複数の端末特定情報とを含み、前記制御部は、前記暗号化コンテンツデータの購入要求に応じて、前記キー操作部を介して入力された購入コンテンツの検索条件を前記送受信部を介して配信サーバへ送信し、前記検索条件に合致するコンテンツのコンテンツ特定情報を前記配信サーバから前記送受信部を介して受信し、その受信したコンテンツ特定情報に一致するコンテンツ特定情報と前記一致したコンテンツ特定情報に対応するライセンス情報および端末特定情報とを前記複数のデータベースおよび前記一覧表から抽出し、その抽出したコンテンツ特定情報、ライセンス情報および端末特定情報を含む検索結果データベースを作成する、情報端末装置。

【請求項 2】 各種の情報を視覚情報としてユーザに与えるための表示部をさらに備え、前記制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を前記検索結果データベースから読出して前記表示部に表示し、前記キー操作部を介して他の情報端末装置が保持する暗号化コンテンツデータの選択が入力されると、前記他の情報端末装置へ前記暗号化コンテンツデータの複製依頼を前記送受信部を介して送信し、前記他の情報端末装置において前記複製が許可されると前記他の情報端末装置から前記暗号化コンテンツデータを前記送受信部を介して受信する、請求項 1 に記載の情報端末装置。

【請求項 3】 前記制御部は、さらに、前記取得要求された暗号化コンテンツデータに対応するライセンス情報がライセンスの無しを表すとき、前記配信サーバから前記複製された暗号化コンテンツデータに対応するライセ

ンスを受信する、請求項 2 に記載の情報端末装置。

【請求項 4】 各種の情報を視覚情報としてユーザに与えるための表示部と、前記データ記録装置との間のやり取りを制御するインタフェースとをさらに備え、前記制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を前記検索結果データベースから読出して前記表示部に表示し、自己がやり取りを行なうデータ記録装置に記録された暗号化コンテンツデータの選択が前記キー操作部を介して入力され、前記選択された暗号化コンテンツデータに対応するライセンス情報がライセンスの無しを表すとき前記ライセンスの送信依頼を前記送受信部を介して前記配信サーバへ送信し、前記配信サーバから前記ライセンスを前記送受信部を介して受信する、請求項 1 に記載の情報端末装置。

【請求項 5】 各種の情報を視覚情報としてユーザに与えるための表示部と、前記データ記録装置との間のやり取りを制御するインタフェースとをさらに備え、前記制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を前記検索結果データベースから読出して前記表示部に表示し、前記配信サーバが保持する暗号化コンテンツデータの選択が前記キー操作部を介して入力されたとき前記選択された暗号化コンテンツデータおよび前記選択された暗号化コンテンツデータに対応するライセンスの送信依頼を前記送受信部を介して前記配信サーバへ送信し、前記配信サーバから前記暗号化コンテンツデータおよびライセンスを前記送受信部を介して受信する、請求項 1 に記載の情報端末装置。

【請求項 6】 前記制御部は、さらに、データベースの取得要求に応じて他の情報端末装置が保持するデータベースを前記他の情報端末装置から前記送受信部を介して受信し、その受信したデータベースを前記記憶部に格納するとともに前記格納したデータベースを追加して前記一覧表を更新する、請求項 1 から請求項 5 のいずれか 1 項に記載の情報端末装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、コンテンツデータを管理するための複数のデータベースを保持し、コンテンツデータの取得要求に応じて複数のデータベースを検索してコンテンツデータを取得する情報端末装置に関するものである。

## 【0002】

【従来の技術】近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがっ

て、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このようなデジタル情報通信網において音楽データや画像データ等の著作権者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度、受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの

配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

10 【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化されたライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

20 【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路を有する。

【0013】各ユーザは、上述したように、自己の携帯電話機によって配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスを自己のメモリカードに記録する。

【0014】

30 【発明が解決しようとする課題】しかし、各ユーザが新たに暗号化コンテンツデータを取得したいとき、その暗号化コンテンツデータが他のユーザのメモリカードに記録されている場合もある。そのような場合、各ユーザは、取得したい暗号化コンテンツデータを配信サーバから受信するのでは、暗号化コンテンツデータの受信に長時間を要し、かつ、通信費も高くなるという問題がある。

【0015】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、ユーザが取得したい暗号化コンテンツデータの格納場所を検索し、その検索した格納場所から暗号化コンテンツデータを取得する情報端末装置を提供することである。

【0016】

40 【課題を解決するための手段】この発明によれば、情報端末装置は、複数の情報端末装置において作成され、かつ、暗号化コンテンツデータを管理するための複数のデータベースを検索して暗号化コンテンツデータと暗号化コンテンツデータを再生するためのライセンスとを取得する情報端末装置であって、外部とのデータのやり取りを行なう送受信部と、指示を入力するためのキー操作部と、複数のデータベースと一覧表とを記憶する記憶部と、制御部とを備え、複数のデータベースの各々は、複

数の暗号化コンテンツデータを特定するための複数のコンテンツ特定情報と、暗号化コンテンツデータに対応するライセンスの有無を示す複数のライセンス情報と、暗号化コンテンツデータおよびライセンスが記録されたデータ記録装置を特定するための複数の記録装置特定情報とを含み、一覧表は、複数のデータベースを特定するための複数のデータベース特定情報と、複数のデータベースの各々が生成された情報端末装置を特定するための複数の端末特定情報とを含み、制御部は、暗号化コンテンツデータの購入要求に応じて、キー操作部を介して入力された購入コンテンツの検索条件を送受信部を介して配信サーバへ送信し、検索条件に合致するコンテンツのコンテンツ特定情報を配信サーバから送受信部を介して受信し、その受信したコンテンツ特定情報に一致するコンテンツ特定情報と一致したコンテンツ特定情報に対応するライセンス情報および端末特定情報とを複数のデータベースおよび一覧表から抽出し、その抽出したコンテンツ特定情報、ライセンス情報および端末特定情報を含む検索結果データベースを作成する。

【0017】好ましくは、情報端末装置は、各種の情報を視覚情報としてユーザに与えるための表示部をさらに備え、制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を検索結果データベースから読出して表示部に表示し、キー操作部を介して他の情報端末装置が保持する暗号化コンテンツデータの選択が入力されると、他の情報端末装置へ暗号化コンテンツデータの複製依頼を送受信部を介して送信し、他の情報端末装置において複製が許可されると他の情報端末装置から暗号化コンテンツデータを送受信部を介して受信する。

【0018】好ましくは、制御部は、さらに、取得要求された暗号化コンテンツデータに対応するライセンス情報がライセンスの無しを表すとき、配信サーバから複製された暗号化コンテンツデータに対応するライセンスを受信する。

【0019】好ましくは、情報端末装置は、各種の情報を視覚情報としてユーザに与えるための表示部と、データ記録装置との間のやり取りを制御するインタフェースとをさらに備え、制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を前記検索結果データベースから読出して表示部に表示し、自己がやり取りを行なうデータ記録装置に記録された暗号化コンテンツデータの選択がキー操作部を介して入力され、選択された暗号化コンテンツデータに対応するライセンス情報がライセンスの無しを表すときライセンスの送信依頼を送受信部を介して配信サーバへ送信し、配信サーバから前記ライセンスを送受信部を介して受信する。

【0020】好ましくは、情報端末装置は、各種の情報を視覚情報としてユーザに与えるための表示部と、データ記録装置との間のやり取りを制御するインタフェースとをさらに備え、制御部は、コンテンツ特定情報、ライ

センス情報、および端末特定情報を検索結果データベースから読出して表示部に表示し、配信サーバが保持する暗号化コンテンツデータの選択がキー操作部を介して入力されたとき選択された暗号化コンテンツデータおよび選択された暗号化コンテンツデータに対応するライセンスの送信依頼を送受信部を介して配信サーバへ送信し、配信サーバから前記暗号化コンテンツデータおよびライセンスを前記送受信部を介して受信する。

【0021】好ましくは、制御部は、さらに、データベースの取得要求に応じて他の情報端末装置が保持するデータベースを他の情報端末装置から送受信部を介して受信し、その受信したデータベースを記憶部に格納するとともに格納したデータベースを追加して一覧表を更新する。

【0022】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0023】図1は、本発明による情報端末装置が暗号化コンテンツデータ、および暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0024】なお、以下では携帯電話網を介して音楽データをユーザの携帯電話機に装着されたメモリカード110～112に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ、ニュース、および英会話用のデータ等を配信する場合においても適用することが可能なものである。

【0025】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。音楽データ等のコンテンツデータを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100（または101、102）に装着されたメモリカード110（または111、112）が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して著作権を保護するために所定の暗号方式によりコンテンツデータを暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータ、付加情報および暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【0026】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100（または101、102）に装着されたメモリカード110（また

は111, 112)に対して、携帯電話網および携帯電話機100(または101, 102)を介して暗号化コンテンツデータとライセンスとを配信する。

【0027】図1においては、たとえば携帯電話ユーザの携帯電話機100(または101, 102)には、着脱可能なメモリカード110(または111, 112)が装着される構成となっている。メモリカード110(または111, 112)は、携帯電話機100(または101, 102)により受信された暗号化コンテンツデータを受取り、著作権を保護するために行なわれた暗号化を復号した上で、携帯電話機100(または101, 102)中の音楽再生部(図示せず)に与える。

【0028】さらに、たとえば携帯電話ユーザは、携帯電話機100(または101, 102)に接続したヘッドホン130(または131, 132)等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0029】このような構成とすることで、まず、メモリカード110(または111, 112)を利用しないと、配信サーバ10からコンテンツデータの配信を受け、音楽を再生することが困難な構成となる。

【0030】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信(ダウンロード)するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0031】したがって、図1に示すデータ配信システムにおいては、携帯電話機100(または101, 102)に装着されたメモリカード110(または111, 112)は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータ、付加情報およびライセンスを受信して格納することができる。

【0032】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信におけるライセンスを配信するための方式であり、さらに第2には、コンテンツデータを暗号化する方式そのものであり、さらに、第3には、このようなコンテンツデータの無断コピーを防止するための著作権保護を実現する構成である。

【0033】また、携帯電話機100~102は、それぞれ、装着されたメモリカード110~112に格納された暗号化コンテンツデータを管理するためのデータベースを後述する方法によって作成し、その作成したデータベースを保持する。さらに、携帯電話機100は、メモリカード111, 112に格納された暗号化コンテンツデータを管理するためのデータベースを携帯電話機101, 102から受信し、メモリカード110に格納さ

れた暗号化コンテンツデータを管理するためのデータベースとともに保持する。つまり、携帯電話機100のユーザは、友人である携帯電話機101, 102のユーザが所有するメモリカード111, 112に格納された暗号化コンテンツデータを管理するためのデータベースを携帯電話機101, 102から受信して保持する。このように、友人が配信サーバ10から受信して自己のメモリカード111, 112に格納した暗号化コンテンツデータを管理するためのデータベースを取得して携帯電話機100に保持することによって、後述するように、携帯電話機100のユーザは、新たな暗号化コンテンツデータを取得したいと思ったとき、その新たな暗号化コンテンツデータが既にメモリカード111, 112へ配信されたものであれば、その新たな暗号化コンテンツデータを携帯電話機101, 102を介してメモリカード111, 112から取得できる。なお、携帯電話機100と携帯電話機101, 102との間の通信は、USB(Universal Serial Bus)ケーブル65を介して行なわれてもよく、無線通信によって行なわれてもよい。

【0034】そして、携帯電話機100は、携帯電話機101, 102から受信した暗号化コンテンツデータを復号および再生するためのライセンスを携帯電話網を介して配信サーバ10から受信する。配信サーバ10は、ライセンスの配信に対して課金を行なうので、ライセンスの取得は原則として配信サーバ10から行なうこととしたものである。

【0035】本発明の実施の形態においては、特に、配信、および再生の各処理の発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証の記録装置および情報端末装置(暗号化コンテンツデータを復号して再生できる再生端末を携帯電話機とも言う。以下同じ)に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0036】なお、以下の説明においては、配信サーバ10から、各携帯電話機に暗号化コンテンツデータ、付加情報、およびライセンスを伝送する処理を「配信」と称することとする。

【0037】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0038】まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ(Dc)Kcがこの形式で配信サーバ10より携帯電話機のユーザに配布される。

【0039】なお、以下においては、{Y}Xという表

記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0040】さらに、配信サーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc-infが配布される。

【0041】また、ライセンスとして、ライセンス鍵Kcと、配信サーバ10からのライセンス鍵等の配信を特定するための管理コードであるライセンスIDとが配信サーバ10と携帯電話機100（または101、102）との間でやり取りされる。さらに、ライセンスとしては、コンテンツデータDcを識別するためのコードであるコンテンツIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ACmおよび情報端末装置における再生に関する制御情報である再生制御情報ACP等が存在する。具体的には、アクセス制御情報ACmは、メモリカードからのライセンスまたはライセンス鍵を外部に出力するに当たっての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報などがある。再生制御情報ACPは、コンテンツデータを再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0042】以後、ライセンスIDと、コンテンツIDと、ライセンス鍵Kcと、アクセス制御情報ACmと、再生制御情報ACPとを併せて、ライセンスと総称することとする。

【0043】図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0044】情報端末装置内のコンテンツ再生デバイス、およびメモリカードには固有の公開暗号鍵KPyおよびKPMwがそれぞれ設けられ、公開暗号鍵KPyおよびKPMwは、コンテンツ再生デバイスに固有の秘密復号鍵Kpy、メモリカードに固有の秘密復号鍵Km wによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、メモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0045】また、コンテンツ再生デバイスのクラス証明書としてCpyが設けられ、メモリカードのクラス証明書としてCmwが設けられる。これらのクラス証明書

は、コンテンツ再生デバイス、およびメモリカードのクラスごとに異なる情報を有する。

【0046】これらのコンテンツ再生デバイスのクラス公開暗号鍵およびクラス証明書は、認証データ{KPy/Cpy} KPaの形式で、メモリカードのクラス公開暗号鍵およびクラス証明書は、認証データ{KPMw/Cmw} KPaの形式で出荷時にデータ再生デバイス、およびメモリカードにそれぞれ記録される。後ほど詳細に説明するが、KPaは配信システム全体で共通の公開認証鍵である。

【0047】また、メモリカード110内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵KPMcxと、公開暗号鍵KPMcxで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Kmcxが存在する。これらのメモリカードごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵KPMcxを個別公開暗号鍵、秘密復号鍵Kmcxを個別秘密復号鍵と称する。

【0048】ライセンスの配信、および再生が行なわれるごとに配信サーバ10、携帯電話機100～102、およびメモリカード110～112において生成される共通鍵Ks1～Ks3が用いられる。

【0049】ここで、共通鍵Ks1～Ks3は、配信サーバ、コンテンツ再生デバイスもしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1～Ks3を「セッションキー」とも呼ぶこととする。

【0050】これらのセッションキーKs1～Ks3は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生デバイス、およびメモリカードによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーKs3は、コンテンツ再生デバイスにおいて再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0051】図4は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツID等の配信情報を保持するための情報データベース304と、携帯電話機の各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、情報データベ

10

20

30

40

50

ス304に保持されたコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0052】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカードから送られてきた認証のための認証データ{Kpmw/Cmw}KPaを復号するための公開認証鍵KPaを保持する認証鍵保持部313と、メモリカードから送られてきた認証のための認証データ{Kpmw/Cmw}KPaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵KPaによって復号処理を行なう復号処理部312と、配信セッションごとに、セッションキーKs1を発生するセッションキー発生部316と、セッションキー発生部316により生成されたセッションキーKs1を復号処理部312によって得られたクラス公開暗号鍵Kpmwを用いて暗号化して、バスBS1に出力するための暗号処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0053】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよびアクセス制御情報ACmを、復号処理部320によって得られたメモリカードごとに個別公開暗号鍵Kpmcxによって暗号化するための暗号処理部326と、暗号処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号処理部328とを含む。

【0054】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0055】図5は、図1に示した携帯電話機100～102の構成を説明するための概略ブロック図である。

【0056】携帯電話機100～102は、携帯電話機100～102の各部のデータ授受を行なうためのバスBS2と、携帯電話網により無線伝送される信号を受信するためのアンテナ1101と、アンテナ1101からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機100～102の各部からのデータを変調して

アンテナ1101に与えるための送受信部1102とを含む。

【0057】携帯電話機100～102は、さらに、暗号化コンテンツデータとともにメモリカード110～112に格納されたコンテンツ管理情報に基づいて作成された、暗号化コンテンツデータを管理するためのデータベースを格納するRAM1103を含む。なお、RAM1103は、他の携帯電話機から取得したデータベースも格納する。

【0058】携帯電話機100～102は、さらに、バスBS2を介して携帯電話機100～102の動作を制御するためのコントローラ1106と、外部からの指示を携帯電話機100～102に与えるためのキー操作部1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるための表示パネル1110とを含む。

【0059】携帯電話機100～102は、さらに、配信サーバ10または他の携帯電話機からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード110～112と、メモリカード110～112とバスBS2との間のデータの授受を制御するためのメモリカードインタフェース1200とを含む。

【0060】携帯電話機100～112は、さらに、クラス公開暗号鍵Kpp1およびクラス証明書Cp1を公開認証鍵KPaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kpp1/Cp1}KPaを保持する認証データ保持部1500を含む。ここで、携帯電話機100～102のクラスyは、y=1であるとする。

【0061】携帯電話機100～102は、さらに、クラス固有の復号鍵であるKp1を保持するKp1保持部1502と、バスBS2から受けたデータをKp1によって復号し、メモリカード110～112によって発生されたセッションキーKs2を得る復号処理部1504とを含む。

【0062】携帯電話機100～102は、さらに、メモリカード110～112に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110～112との間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110～112からライセンス鍵Kcおよび再生制御情報ACpを受取る際に、セッションキー発生部1508により発生されたセッションキーKs3を復号処理部1504によって得られたセッションキーKs2によって暗号化し、バスBS2に出力する暗号処理部1506とを含む。

【0063】携帯電話機100～102は、さらに、バ

スBS2上のデータをセッションキーKs3によって復号して、ライセンス鍵Kcおよび再生制御情報ACpを出力する復号処理部1510と、バスBS2より暗号化コンテンツデータ{Dc}Kcを受けて、復号処理部1510からのライセンス鍵Kcによって暗号化コンテンツデータ{Dc}Kcを復号してコンテンツデータDcを音楽再生部1518へ出力する復号処理部1516とを含む。

【0064】携帯電話機100～102は、さらに、復号処理部1516からの出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518の出力をデジタル信号からアナログ信号に変換するDA変換器1519と、DA変換器1519の出力をヘッドホンなどの外部出力装置(図示省略)へ出力するための端子1530とを含む。

【0065】携帯電話機100～102は、さらに、他の携帯電話機からコンテンツデータ、付加情報およびライセンスを受信する際にバスBS2と端子1114との間のデータ授受を制御するためのUSBインタフェース1112と、USBケーブル65を接続するための端子1114とを含む。

【0066】また、図5においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス1550を構成する。

【0067】さらに、図5においては、通常の通話機能に必要な音声データの変調および復号を行なう音声コーデック、およびマイク等は省略している。

【0068】携帯電話機100～102の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0069】図6は、図1に示すメモリカード110～112の構成を説明するための概略ブロック図である。

【0070】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、KpmwおよびKmwが設けられ、メモリカードのクラス証明書Cmwが設けられるが、メモリカード110においては、自然数w=3で表わされるものとする。また、メモリカードを識別する自然数xは、メモリカード110に対してはx=4で表わされるものとする。

【0071】したがって、メモリカード110は、認証データ{Kpm3/／Cm3}KPaを保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Kmc4を保持するKmc保持部1402と、クラス秘密復号鍵Km3を保持するKm保持部1421と、個別秘密復号鍵Kmc4によって復号可能な公開暗号鍵Kpmc4を保持するKpmc保持部1416とを含む。

【0072】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化され

たライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0073】メモリカード110は、さらに、メモリカードインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS3と、バスBS3にインタフェース1424から与えられるデータから、クラス秘密復号鍵Km3をKm保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1422と、KPa保持部1414から公開認証鍵KPaを受けて、バスBS3に与えられるデータの公開認証鍵KPaによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ1420に、得られたクラス公開鍵を暗号処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS4に出力する暗号処理部1406とを含む。

【0074】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られるクラス公開暗号鍵KppyもしくはKpmwによって暗号化してバスBS3に出力する暗号処理部1410と、バスBS3よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号する復号処理部1412と、暗号化コンテンツデータの再生セッションにおいてメモリ1415から読出されたライセンス鍵Kcおよび再生制御情報ACpを、復号処理部1412で復号された他のメモリカード110の個別公開暗号鍵Kpmcx(x≠4)で暗号化する暗号処理部1417とを含む。

【0075】メモリカード110は、さらに、バスBS3上のデータを個別公開暗号鍵Kpmc4と対をなすメモリカード110の個別秘密復号鍵Kmc4によって復号するための復号処理部1404と、配信サーバ10との間の通信における履歴を格納するログと、暗号化コンテンツデータ{Dc}Kcと、暗号化コンテンツデータ{Dc}Kcを再生するためのライセンス(Kc, ACp, ACm, ライセンスID, コンテンツID)と、付加情報Dc-infと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスBS3より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1415は、ログ領域1415Aと、ライセンス領域1415Bと、データ領域1415Cとから成る。ログ領域1415Aは、ログを記録するための領域である。ログ領域141

5Aは、メモリカード110に対してライセンスが入力され、格納されるときに記録される受信ログを含む。

【0076】ライセンス領域1415Bは、ライセンスを記録するための領域である。ライセンス領域1415Bは、ライセンス（ライセンス鍵Kc、再生制御情報ACp、アクセス制限情報ACm、ライセンスID、コンテンツID）を格納する。ライセンスは、エントリ番号に対応してライセンス領域1415Bに格納されており、ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【0077】データ領域1415Cは、暗号化コンテンツデータ{Dc}Kc、暗号化コンテンツデータの付加情報Dc-inf、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストを記録するための領域である。そして、データ領域1415Cは、外部から直接アクセスすることができる。

【0078】メモリカード110は、さらに、バスBS3を介して外部との間でデータ授受を行ない、バスBS3との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420を含む。

【0079】なお、データ領域1415Cを除く全ての構成は、耐タンパモジュール領域に構成される。

【0080】また、メモリカード111、112は、メモリカード110と同じ構成からなる。この場合、メモリカードを識別するための自然数xは、「4」以外の自然数が用いられる。

【0081】以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0082】〔配信〕まず、図1に示すデータ配信システムにおいて、配信サーバ10から携帯電話機100のメモリカード110へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。

【0083】図7および図8は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機100に装着されたメモリカード110への暗号化コンテンツデータ{Dc}Kc、付加情報Dc-inf、およびライセンスの配信動作（以下、配信セッションともいう）を説明するための第1および第2のフローチャートである。

【0084】図7における処理以前に、携帯電話機100のユーザは、配信サーバ10に対して携帯電話網を介して接続し、購入を希望するコンテンツに対するコンテンツIDを取得していることを前提としている。

【0085】図7を参照して、携帯電話機100のユーザからキー操作部1108を介してコンテンツIDの指

定による配信リクエストがなされる（ステップS100）。そして、キー操作部1108を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACを入力するように指示し、購入条件ACが入力される（ステップS102）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータのアクセス制御情報ACm、および再生制御情報ACpを設定して購入条件ACが入力される。

10 【0086】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ1106は、バスBS2およびメモリカードインタフェース1200を介してメモリカード110へ認証データの出力指示を与える（ステップS104）。メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して認証データの送信要求を受信する（ステップS106）。そして、コントローラ1420は、バスBS3を介して認証データ保持部1400から認証データ{Kpm3/Cm3}KPaを読み出し、20 {Kpm3/Cm3}KPaをバスBS3、インタフェース1424および端子1426を介して出力する（ステップS108）。

【0087】携帯電話機100のコントローラ1106は、メモリカード110からの認証データ{Kpm3/Cm3}KPaに加えて、コンテンツID、ライセンス購入条件のデータAC、および配信リクエストを配信サーバ10に対して送信する（ステップS110）。

【0088】配信サーバ10では、携帯電話機100から配信リクエスト、コンテンツID、認証データ{Kpm3/Cm3}KPa、およびライセンス購入条件のデータACを受信し（ステップS112）、復号処理部312においてメモリカード110から出力された認証データを公開認証鍵KPaで復号処理を実行する（ステップS114）。

【0089】配信制御部315は、復号処理部312における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップS116）。正当な認証データであると判断された場合、配信制御部315は、クラス公開暗号鍵Kpm3およびクラス証明書Cm3を承認し、受理する。そして、次の処理（ステップS118）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵Kpm3およびクラス証明書Cm3を受理しないで配信セッションを終了する（ステップS184）。

【0090】認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ10において、セッションキー発生部316は、配信のためのセッションキーKs1を生成する（ステップS118）。セッションキー

Ks1は、復号処理部312によって得られたメモリカード110に対応するクラス公開暗号鍵Kpm3によって、暗号処理部318によって暗号化される(ステップS120)。

【0091】配信制御部315は、ライセンスIDを生成し(ステップS122)、ライセンスIDおよび暗号化されたセッションキーKs1は、ライセンスID/{Ks1}Km3として、バスBS1および通信装置350を介して外部に出力される(ステップS124)。

【0092】携帯電話機100が、ライセンスID/{Ks1}Km3を受信すると、コントローラ1106は、ライセンスID/{Ks1}Km3をメモリカード110に入力する(ステップS126)。そうすると、メモリカード110においては、端子1426およびインタフェース1424を介して、コントローラ1420は、ライセンスID/{Ks1}Km3を受信する(ステップS128)。そして、コントローラ1420は、バスBS3を介してメモリ1415のログ領域1415Aに記録されている受信ログを初期化し、受理したライセンスIDをログ領域1415Aに格納する(ステップS130)。このとき、受信ログ内の受信stateは、OFFに設定される。その後、コントローラ1420は、バスBS3を介して{Ks1}Km3を復号処理部1422に与え、復号処理部1422は、Km保持部1421に保持されるメモリカード110に固有なクラス秘密復号鍵Km3によって{Ks1}Km3を復号処理することにより、セッションキーKs1を復号し、セッションキーKs1を受信する(ステップS132)。

【0093】コントローラ1420は、配信サーバ10で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対してメモリカード110において配信動作時に生成されるセッションキーKs2の生成を指示する。そして、セッションキー発生部1418は、セッションキーKs2を生成する(ステップS134)。コントローラ1420は、生成されたセッションキーKs2をバスBS3を介して受取り、その受取ったセッションキーKs2をメモリ1415のログ領域1415Aに格納し、受信stateをONにする(ステップS136)。

【0094】暗号処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1422より与えられるセッションキーKs1によって、切換スイッチ1446の接点を順次切換えることによって与えられるセッションキーKs2、および個別公開暗号鍵Kpmc4を1つのデータ列として暗号化して、{Ks2//Kpmc4}Ks1をバスBS3に出力する。バスBS3に出力された暗号化データ{Ks2//Kpmc4}Ks1は、バスBS3からインタフェース1424および端子1426を介して携帯電話機100に出力され(ステッ

プS138)、携帯電話機100から配信サーバ10に送信される(ステップS140)。

【0095】図8を参照して、配信サーバ10は、{Ks2//Kpmc4}Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、およびメモリカード110の個別公開暗号鍵Kpmc4を受信する(ステップS142)。

【0096】配信制御部315は、ステップS112で取得したコンテンツIDに従ってライセンス鍵Kcを情報データベース304から取得し(ステップS144)、ステップS112で取得したライセンス購入条件のデータACに従って、アクセス制御情報ACmおよび再生制御情報ACpを決定する(ステップS146)。

【0097】配信制御部315は、生成したライセンス、すなわち、ライセンスID、コンテンツID、ライセンス鍵Kc、再生制御情報ACp、およびアクセス制御情報ACmを暗号処理部326に与える。暗号処理部326は、復号処理部320によって得られたメモリカード110の個別公開暗号鍵Kpmc4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Km4c4を生成する(ステップS148)。そして、暗号処理部328は、暗号処理部326からの暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Km4c4を、復号処理部320からのセッションキーKs2によって暗号化し、暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Km4c4}Ks2を出力する。配信制御部315は、バスBS1および通信装置350を介して暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Km4c4}Ks2を携帯電話機100へ送信する(ステップS150)。

【0098】携帯電話機100は、送信された暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Km4c4}Ks2を受信し、バスBS2を介してメモリカード110に入力する(ステップS152)。メモリカード110においては、端子1426およびインタフェース1424を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS3上の受信データを復号し、バスBS3に出力する(ステップS154)。

【0099】この段階で、バスBS3には、Km保持部1402に保持される個別秘密復号鍵Km4c4で復号可能な暗号化ライセンス{ライセンスID//コンテンツID//Kc//ACm//ACp}Km4c4が出力される(ステップS154)。

【0100】コントローラ1420の指示によって、暗

10

20

30

40

50

号化ライセンス（ライセンスID／コンテンツID／Kc／ACm／ACp）Kmc4は、復号処理部1404において、個別秘密復号鍵Kmc4によって復号され、ライセンス（ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp）が受理される（ステップS156）。そして、この段階で携帯電話機100のコントローラ1106から端子1426およびインタフェース1424を介してライセンスを格納するためのエントリ番号が入力される。

【0101】そうすると、コントローラ1420は、受理したライセンス（ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp）を受理したエントリ番号に従ってメモリ1415のライセンス領域1415Bに格納する（ステップS158）。そして、コントローラ1420は、バスBS3を介してメモリ1415のログ領域1415Aの受信ログに記録された受信stateをOFFする（ステップS160）。ライセンスの書き込みが終了すると、携帯電話機100のコントローラ1106は、ライセンス管理情報を更新し、その更新したライセンス管理情報をメモリカード110へ入力する（ステップS162）。メモリカード110のコントローラ1420は、入力されたライセンス管理情報をメモリ1415のデータ領域1415Cに書込む（ステップS164）。

【0102】ライセンスの配信が終了した後、携帯電話機100のコントローラ1106は、暗号化コンテンツデータの配信要求を配信サーバ10へ送信し（ステップS166）、配信サーバ10は、暗号化コンテンツデータの配信要求を受信する（ステップS168）。そして、配信サーバ10の配信制御部315は、情報データベース304より、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する（ステップS170）。

【0103】携帯電話機100は、{Dc}Kc／Dc-infを受信して、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受理する（ステップS172）。そうすると、コントローラ1106は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infをバスBS2およびメモリカードインタフェース1200を介してメモリカード110へ入力する（ステップS174）。

【0104】メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受信し、その受理した暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infをメモリ1415のデータ領域1415Cに記録する（ステップS176）。そして、コントローラ1

420は、受理したコンテンツの情報をデータ領域1415Cの再生リストに追記する（ステップS178）。【0105】そうすると、携帯電話機100のコントローラ1106は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infの配信受理を配信サーバ10へ送信し（ステップS180）、配信サーバ10は、配信受理を受信し、配信制御部315は、バスBS1を介して課金データベース302に書込んで課金処理を行なう（ステップS182）。そして、配信動作が終了する（ステップS184）。

【0106】このようにして、携帯電話機100に装着されたメモリカード110が正規の認証データを保持する機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵Kpm3が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

【0107】また、携帯電話機101、102に装着されたメモリカード111、112への暗号化コンテンツデータ、付加情報、およびライセンスの配信も図7および図8に示すフローチャートに従って行なわれる。

【0108】図9は、メモリカード110のメモリ1415におけるライセンス領域1415Bとデータ領域1415Cとを示したものである。データ領域1415Cには、再生リストファイル160と、エントリ管理情報165と、カードID166と、コンテンツファイル1611～161nと、ライセンス管理ファイル1621～162nとが記録されている。コンテンツファイル1611～161nは、受信した暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを1つのファイルとして記録する。また、ライセンス管理ファイル1621～162nは、それぞれ、コンテンツファイル1611～161nに対応して記録され、対応するコンテンツファイル1611～161nに記録された暗号化コンテンツデータを復号および再生するためのライセンスが格納されたエントリ番号を含む。

【0109】ライセンス領域1415Bは、エントリ番号によって指定された領域にライセンスと有効フラグとを格納する。したがって、ライセンス管理ファイル1621～162nからエントリ番号を読出せば、その読出したエントリ番号によってライセンス管理ファイル1621～162nに対応するコンテンツファイル1611～161nに記録された暗号化コンテンツデータを復号するためのライセンスをライセンス領域1415Bから読出することができる構成になっている。また、有効フラグは、ライセンスをメモリカード110から外部へ出すことができるか否かを示すものであり、メモリカード110にライセンスが格納されているときは「有効」と記録され、後述するライセンスの移動によってライセンスをメモリカード110から外部へ出したときは「無効」

10

20

30

40

50

と記録される。

【0110】メモリカード110は、配信サーバ10から暗号化コンテンツデータおよびライセンスを受信したとき、暗号化コンテンツデータおよびライセンスをメモリ1415に記録する。

【0111】また、ライセンス管理ファイル1622は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル1612は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、携帯電話機が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

【0112】図10は、図9に示すコンテンツファイル1611~161nに記録された暗号化コンテンツデータ(Dc)Kcと付加情報Dc-infとの関係を示す概念図である。なお、図10は、コンテンツ数が10個の場合を示す。コンテンツデータ1631~1640は、それぞれ、コンテンツファイル1611~1620に記録された暗号化コンテンツデータである。コンテンツ管理情報163は、管理情報1651~1660から成り、管理情報1651~1660は、コンテンツID、タイトル名、アーティスト名およびコンテンツ種別を含む。そして、管理情報1651~1660は、それぞれ、コンテンツデータ1631~1640を管理するための管理情報である。したがって、管理情報1651~1660は、それぞれ、コンテンツデータ1631~1640に対応付けられてコンテンツ管理情報163を構成する。

【0113】[再生]携帯電話機100に装着されたメモリカード110が、配信サーバ10から受信した暗号化コンテンツデータの再生動作について説明する。

【0114】図11は、メモリカード110が受信したコンテンツデータの携帯電話機100における再生動作を説明するためのフローチャートである。なお、図11における処理以前に、携帯電話機100のユーザは、メモリカード100のデータ領域1415Cに記録されている再生リストに従って、再生するコンテンツ(楽曲)を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提としている。

【0115】図11を参照して、再生動作の開始とともに、携帯電話機100のユーザからキー操作部1108を介して再生リクエストが携帯電話機100にインプットされる(ステップS700)。そうすると、コントローラ1106は、バスBS2を介して認証データの出力要求をコンテンツ再生デバイス1550に行ない(ステップS702)、コンテンツ再生デバイス1550は認証データの出力要求を受信する(ステップS704)。そして、認証データ保持部1500は、認証データ(KPp1/Cp1)KPaを出力し(ステップS706)、コントローラ1106は、メモリカードインタフ

ェース1200を介してメモリカード110へ認証データ(KPp1/Cp1)KPaを入力する(ステップS708)。

【0116】そうすると、メモリカード110は、認証データ(KPp1/Cp1)KPaを受理し、復号処理部1408は、受理した認証データ(KPp1/Cp1)KPaを、KPa保持部1414に保持された公開認証鍵KPaによって復号し(ステップS710)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ(KPp1/Cp1)KPaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS712)。復号できなかった場合、ステップS746へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ1420は、セッションキー発生部1418を制御し、セッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS713)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵KPp1によって暗号化した(Ks2)Kp1をバスBS3へ出力する。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ(Ks2)Kp1を出力する(ステップS714)。携帯電話機100のコントローラ1106は、メモリカードインタフェース1200を介して(Ks2)Kp1を取得する。そして、コントローラ1106は、(Ks2)Kp1をバスBS2を介してコンテンツ再生デバイス1550の復号処理部1504へ与え(ステップS716)、復号処理部1504は、Kp1保持部1502から出力された、公開暗号鍵KPp1と対になっている秘密復号鍵Kp1によって(Ks2)Kp1を復号し、セッションキーKs2を暗号処理部1506へ出力する(ステップS718)。そうすると、セッションキー発生部1508は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1506へ出力する(ステップS720)。暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3を復号処理部1504からのセッションキーKs2によって暗号化して(Ks3)Ks2を出力し(ステップS722)、コントローラ1106は、バスBS2およびメモリカードインタフェース1200を介して(Ks3)Ks2をメモリカード110へ出力する(ステップS724)。

【0117】そうすると、メモリカード110の復号処理部1412は、端子1426、インタフェース1424、およびバスBS3を介して(Ks3)Ks2を入力する。復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーKs2によっ

て(Ks3) Ks2を復号して、携帯電話機100で発生されたセッションキーKs3を受理する(ステップS726)。

【0118】携帯電話機100のコントローラ1106は、メモリカード110から事前取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し(ステップS728)、その取得したエントリ番号と再生許諾要求とをメモリカードインタフェース1200を介してメモリカード110へ出力する(ステップS730)。

【0119】メモリカード110のコントローラ1420は、エントリ番号と再生許諾要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスおよび有効フラグを取得する(ステップS732)。そして、コントローラ1420は、有効フラグを確認する(ステップS733)。ステップS733において、有効フラグが「無」の場合、指定されたエントリにライセンスが存在しないので、再生動作が終了する(ステップS746)。ステップS733において、有効フラグが「有効」の場合、指定されたエントリにライセンスが存在するので次のステップS734へ進む。

【0120】そして、コントローラ1420は、アクセス制限情報ACmを確認する(ステップS734)。

【0121】ステップS734においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ACmを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ACmの再生回数を変更し(ステップS736)、次のステップに進む(ステップS738)。一方、アクセス制限情報ACmの再生回数によって再生が制限されていない場合においては、ステップS736はスキップされ、アクセス制限情報ACmの再生回数は変更されことなく処理が次のステップ(ステップS738)に進行される。

【0122】ステップS734において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415Bに記録された再生リクエスト曲のライセンス鍵Kcおよび再生制御情報ACpがバスBS3上に出力される(ステップS738)。

【0123】得られたライセンス鍵Kcと再生制御情報ACpは、切換スイッチ1446の接点Pfを介して暗号処理部1406に送られる。暗号処理部1406は、切換スイッチ1442の接点Pbを介して復号処理部1412より受けたセッションキーKs3によって切換スイッチ1446を介して受けたライセンス鍵Kcと再生制御情報ACpとを暗号化し、{Kc//ACp} Ks3をバスBS3に出力する(ステップS738)。

【0124】バスBS3に出力された暗号化データは、

インタフェース1424、端子1426、およびメモリカードインタフェース1200を介して携帯電話機100に送出される。

【0125】携帯電話機100においては、メモリカードインタフェース1200を介してバスBS2に伝達される暗号化データ{Kc//ACp} Ks3を復号処理部1510によって復号処理を行ない、ライセンス鍵Kcおよび再生制御情報ACpを受理する(ステップS740、S742)。復号処理部1510は、ライセンス鍵Kcを復号処理部1516に伝達し、再生制御情報ACpをバスBS2に出力する。

【0126】コントローラ1106は、バスBS2を介して、再生制御情報ACpを受理して再生の可否を確認する(ステップS744)。

【0127】ステップS744においては、再生制御情報ACpによって再生不可と判断される場合には、再生動作は終了される。

【0128】ステップS744において再生可能と判断された場合、コントローラ1106は、バスBS2およびメモリカードインタフェース1200を介してメモリカード110に暗号化コンテンツデータ{Dc} Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Dc} Kcを取得し、バスBS3、インタフェース1424、および端子1426を介してメモリカードインタフェース1200へ出力する。

【0129】携帯電話機100のコントローラ1106は、メモリカードインタフェース1200およびバスBS2を介して暗号化コンテンツデータ{Dc} Kcを取得し、バスBS2を介して暗号化コンテンツデータ{Dc} Kcをコンテンツ再生デバイス1550へ与える。

【0130】そして、コンテンツ再生デバイス1550の復号処理部1516は、暗号化コンテンツデータ{Dc} Kcを復号処理部1510から出力されたライセンス鍵Kcによって復号してコンテンツデータDcを取得する。

【0131】そして、復号されたコンテンツデータDcは音楽再生部1518へ出力され、音楽再生部1518は、コンテンツデータ{Dc} Kcを再生し、DA変換器1519はデジタル信号をアナログ信号に変換して端子1530へ出力する。そして、音楽データは端子1530から外部出力装置を介してヘッドホン130へ出力されて再生される。これによって再生動作が終了する(ステップS746)。

【0132】メモリカード111、112に記録された暗号化コンテンツデータのそれぞれ携帯電話機101、102における再生動作も図11に示すフローチャートに従って行なわれる。

【0133】携帯電話機100~102は、それぞれ、メモリカード110~112が装着されると、メモリカ

10

20

30

40

50

ード110~112に記録された暗号化コンテンツデータを管理するためのデータベースを作成し、その作成したデータベースをRAM1103に格納する。図12を参照して、携帯電話機100~102におけるデータベースの作成について説明する。

【0134】図12を参照して、データベース150は、コンテンツNo1531、コンテンツID1532、タイトル名1533、アーティスト名1534、コンテンツ種別1535、ライセンス有無1536、および格納カードID1537を含む。携帯電話機100のコントローラ1106は、メモリカード110が装着されると、バスBS2およびメモリカードインタフェース1200を介してメモリカード110のメモリ1415のデータ領域1415Cから付加情報Decinf、エントリ番号およびカードIDを読み出す。そして、読出した付加情報Decinfに含まれるコンテンツID、タイトル名、アーティスト名、およびコンテンツ種別を、それぞれ、データベース150のコンテンツNo1531、コンテンツID1532、タイトル名1533、アーティスト名1534、およびコンテンツ種別1535に格納する。また、コントローラ1106は、読出したエントリ番号に基づいて対応するコンテンツデータのライセンスの有無をライセンス有無1536に格納する。すなわち、コントローラ1106は、メモリカード110からエントリ番号を読み出すことができれば、ライセンスが有ると認識し、エントリ番号を読み出すことができない場合は、ライセンスが無いと認識する。また、コントローラ1106は、メモリカード110から読出したカードIDを格納カードID1537に格納する。

【0135】コントローラ1106は、携帯電話機100に複数のメモリカードが、順次、装着された場合、その全てのメモリカードに格納されている暗号化コンテンツデータについてのデータベースを作成する。したがって、図12においては、格納カードID1537には、複数のカードIDが示されており、コンテンツNo1531が1~Nのコンテンツは、相互に異なるメモリカードに格納されていることを表している。そして、コントローラ1106は、作成したデータベース150をRAM1103に格納する。

【0136】携帯電話機101、102も、携帯電話機100の場合と同様にして装着されたメモリカードに格納された暗号化コンテンツデータを管理するためのデータベースを作成し、その作成したデータベースをRAM1103に格納する。

【0137】図13および図14を参照して、携帯電話機100が配信サーバ10から受信した暗号化コンテンツデータおよびライセンスをメモリカード110に記録し、メモリカード110に記録した暗号化コンテンツデータを管理するためのデータベースを作成した段階で携帯電話機100のユーザが可能な動作について説明す

る。この段階で、携帯電話機100の表示パネル1110には、図13に示す画面170が表示されている。

【0138】携帯電話機100のユーザは、友人である携帯電話機101、102のユーザから携帯電話機101、102のRAM1103に格納されたデータベースを送信して貰うことが可能である。

【0139】図13を参照して、携帯電話機100のユーザは、表示パネル1110の画面170を見て、「所有曲情報の取得」を選択し、「決定」を押すと表示パネル1110には、画面171が表示される。画面171は、携帯電話機101、102からデータベースを送信して貰うときの通信方法を携帯電話機100のユーザに問う画面である。携帯電話機100のユーザは、たとえば、「ケーブル接続」を選択して「決定」を押す。そうすると、表示パネル1110には、「ケーブルを接続して「開始」を押してください」とのコメントの画面172が表示される。携帯電話機100のユーザは、自己の携帯電話機100をケーブルによって携帯電話機101、102と接続して「開始」を押す。

【0140】そして、表示パネル1110には、「取得中・・・」のメッセージを示す画面173が表示される。所有曲情報の取得が終了すると、表示パネル1110には、取得が完了した旨のメッセージを示す画面174が表示される。このようにして、携帯電話機100のユーザは、携帯電話機101、102からデータベースを受信する。そして、携帯電話機100のコントローラ1106は、受信したデータベースをRAM1103に格納する。したがって、RAM1103には、図12に示すようなデータベースが複数個格納される。携帯電話機100のコントローラ1106は、RAM1103に複数のデータベースが格納されると、図15に示すような複数のデータベースを管理するための一覧表155を作成し、RAM1103に格納する。

【0141】一覧表155は、データベースNo1551、コンテンツデータベース1552、コンテンツ数1553、端末ID1554、および所有者名1555を含む。データベースNo1551は、各データベースに付与される整理番号である。なお、「1」は、自己の携帯電話機に保持されたデータベースであることを示す。コンテンツデータベース1552は、複数のデータベースを識別ための情報である。コンテンツ数1553は、各データベースに含まれるコンテンツ数を示す。端末ID1554は、各データベースを保持する携帯電話機を特定する情報である。端末IDとしては、たとえば、携帯電話機の電話番号が考えられる。所有者名1555は、各データベースの所有者を表す。

【0142】このように、携帯電話機100のコントローラ1106は、携帯電話機101、102からデータベースを受信すると、一覧表155を作成し、その作成した一覧表155をRAM1103に格納する。

【0143】再び、図13を参照して、携帯電話機100のユーザが画面170において、「曲の購入」を選択して「決定」を押すと、画面175が表示パネル1110に表示される。つまり、新たに購入したい曲の検索方法を携帯電話機100のユーザに問う画面が表示される。携帯電話機100のユーザは、「アーティスト名」を選択して「決定」を押すと、検索したいアーティスト名の入力を促す画面176が表示パネル1110に表示される。

【0144】携帯電話機100のユーザは、「アーティストA」を入力して「検索開始」を押す。入力された「アーティストA」は携帯電話機100から配信サーバ10へ送信される。そして、配信サーバ10は、携帯電話機100から受信した「アーティストA」によってアーティストAが作曲した音楽データのコンテンツIDとタイトル名とを検索し、その検索結果を携帯電話機100へ送信する。

【0145】そうすると、携帯電話機100においては、検索結果を配信サーバ10から受信し、アーティストAが作曲した曲のタイトル名、その曲を所有している者、その曲のライセンスがその曲を格納している場所是否存在するか否かを示す情報が画面177として表示パネル1110に表示される。

【0146】画面177が表示パネル1110に表示された時点で、携帯電話機100のユーザが「タイトル4」の曲を選択すると、表示パネル1110に画面178が表示される。「タイトル4」の曲は、Bさんが所有しており、ライセンスが無いので、Bさんの携帯電話機を介してBさんのメモリカードに格納された暗号化コンテンツデータをコピー（複製）することになる。そこで、次に、表示パネル1110にBさんの携帯電話機から暗号化コンテンツデータをコピーするときの通信方法を問合わせる画面178が表示される。携帯電話機100のユーザは、画面178において、「ケーブル接続」を選択して「決定」を押すと、「ケーブルを接続して準備ができたなら「開始」を押してください。」とのメッセージが表示される（画面179）。携帯電話機100のユーザは、自己の携帯電話機100をケーブルによってBさんの携帯電話機と接続し、「開始」を押す。

【0147】図14を参照して、表示パネル1110には、「コピー許可の問合わせ中」のメッセージが表示される（画面180）。Bさんがタイトル4のコンテンツが格納されているメモリカードを装着してコピーを許可すると、「コピーが許可され、タイトル4のコンテンツをコピーしています」というメッセージとコピーの進行状況とが表示パネル1110に表示される（画面181）。Bさんのメモリカードから暗号化コンテンツデータのコピーが終了すると、「「タイトル4」の取得に成功した」ことを示すメッセージが表示されるとともに、「ライセンスを取得する場合には、「ライセンスの取

得」を押してください」とのメッセージが表示される（画面182）。そして、携帯電話機100のユーザが「ライセンスの取得」を押すと、画面183に移行する。

【0148】図13に示す画面177において、「タイトル3」を選択した場合、「タイトル3」のコンテンツは、携帯電話機100のユーザに保持され、ライセンスが無いので、図14に示す画面183に移行する。

【0149】画面183においては、「配信サーバ10に接続して「タイトルn」のライセンスを取得しています」というメッセージが表示パネル1110に表示される（画面183）。そして、ライセンスの取得が終了すると、「「タイトルn」のライセンスの取得が完了いたしました」というメッセージが表示パネル1110に表示される（画面184）。なお、図13に示す画面177において、携帯電話機100のユーザが「タイトル2」を選択した場合、「タイトル2」のコンテンツおよびライセンスは、携帯電話機100のユーザに保持されているので、暗号化コンテンツデータのコピーまたはライセンスの配信サーバ10からの受信は行なわれない。また、画面177において、携帯電話機100～102に装着されるメモリカード110～112に配信されていない暗号化コンテンツデータが選択された場合、図7および図8に示すフローチャートに従って暗号化コンテンツデータおよびライセンスの配信動作が実行される。

【0150】携帯電話機100は、他の携帯電話機から暗号化コンテンツデータをコピーし、そのコピーした暗号化コンテンツデータのライセンスを配信サーバ10から受信したとき、暗号化コンテンツデータおよびライセンスをメモリカード110に記録するとともに、メモリカード110に格納されている暗号化コンテンツデータを管理するためのデータベースを更新する。

【0151】図16および図17を参照して、図13に示す画面175～177における動作を詳細に説明する。図16は、配信サーバ10における暗号化コンテンツデータの検索動作を説明するためのフローチャートである。また、図17は、配信サーバ10における検索結果を受信した携帯電話機100が、検索結果に記載された暗号化コンテンツデータを自己が保持するデータベースに基づいて検索する動作を説明するためのフローチャートである。

【0152】図16を参照して、検索動作が開始されると、携帯電話機100のユーザは、アーティストAをキー操作部1108から入力してコンテンツの検索を配信サーバ10へ問合わせる（ステップS200）。配信サーバ10は、携帯電話機100からアーティストAを受信し、配信制御部315は、バスBS1を介して情報データベース304に格納された暗号化コンテンツデータの付加情報Dc i n fに基づいてアーティストAのコンテンツを検索し、その検索結果をバスBS1および

通信装置350を介して携帯電話機100へ送信する。この場合、配信サーバ10は、図18に示すようなコンテンツ数S、コンテンツID、およびタイトル名の一覧表を検索結果として携帯電話機100へ送信する。

【0153】そうすると、携帯電話機100のコントローラ1106は、アンテナ1101および送受信部1102を介して検索結果を受信し、配信サーバ10で検出されたコンテンツ数Sを取得して検索結果のコンテンツ数をSに設定する(ステップS202)。そして、コントローラ1106は、検索結果データベースを作成する(ステップS204)。つまり、コントローラ1106は、図19に示すように配信サーバ10において検索されたコンテンツ数をSに設定した検索結果データベースを作成する。

【0154】その後、コントローラ1106は、配信サーバ10から受信した検索結果(図18参照)のコンテンツIDおよびタイトル名を取得し、図19に示す検索結果データベースのコンテンツIDの欄およびタイトル名の欄に、それぞれ、取得したコンテンツIDおよびタイトル名を格納する(ステップS206)。そして、コントローラ1106は、検索結果データベース(図19参照)の所有端末数の欄および所有端末IDの欄を全て「0」に初期化する(ステップS208)。コントローラ1106は、さらに、検索結果データベースのライセンス有無の欄を全て「0」に初期化して(ステップS210)、コンテンツの検索動作が終了する。

【0155】その後、図17に示すフローチャートが実行される。携帯電話機100が配信サーバ10から受信した検索結果(図18参照)に含まれるコンテンツID(1)~コンテンツID(S)によって特定されるコンテンツを、携帯電話機100のRAM1103に格納されたデータベースを参照して検索する動作が開始されると、 $m=1$ に設定され(ステップS300)、 $n=1$ に設定され(ステップS302)、 $s=1$ に設定される(ステップS304)。ここで、 $m$ は、RAM1103に格納されたデータベースの数を表し、 $n$ は、各データベースに含まれるコンテンツ数を表し、 $s$ は、検索結果データベース(図19参照)に含まれるコンテンツ数を表す。

【0156】ステップS304の後、携帯電話機100のコントローラ1106は、検索結果データベースのコンテンツID(1)がRAM1103に格納されたデータベース(1)に含まれるコンテンツIDに一致するか否かを判定する(ステップS306)。ステップS306において、検索結果データベースのコンテンツID(1)がデータベース(1)に含まれるコンテンツIDに一致すると判定されたとき、コントローラ1106は、データベース(1)を保持する端末IDをRAM1103に格納された一覧表155(図15参照)から読み出し、その読み出した端末IDを検索結果データベースの

所有端末IDの欄に格納する(ステップS308)。また、コントローラ1106は、データベース(1)(図12参照)からコンテンツID(1)に対応するライセンス有無を読み出し、その読み出したライセンス有無を検索結果データベースのライセンス有無の欄に格納する(ステップS310)。その後、ステップS312へ移行する。

【0157】また、ステップS306において、検索結果データベースのコンテンツID(1)がデータベース(1)に含まれるコンテンツIDに一致しないと判定されたときもステップS312へ移行する。ステップS312において、 $s=s+1$ に設定され(ステップS312)、コントローラ1106は、 $s=S$ か否かを判定する(ステップS314)。ここで、 $S$ は、配信サーバ10において検索されたコンテンツの総数である(図19参照)。ステップS314において $s=S$ であると判定されたとき、ステップS316へ移行する。また、ステップS314において $s=S$ でないと判定されたとき、ステップS306~S314が繰返される。すなわち、ステップS306~S314は、検索結果データベースに含まれるコンテンツID(1)~コンテンツID

(S)がデータベース(1)に含まれるコンテンツID(1)に一致するか否かを判定し、一致すれば、その一致したコンテンツID(1)に対応するライセンスの有無とコンテンツID(1)を含むデータベースを保持する端末IDとをRAM1103に格納されたデータベース(図12参照)および一覧表(図15参照)から読み出し、検索結果データベースに格納するステップである。

【0158】ステップS314において、 $s=S$ であると判定されたとき、 $n=n+1$ に設定され、コントローラ1106は、 $n=N(m)$ であるか否かを判定する(ステップS318)。ステップS318において $n=N(m)$ でないと判定されたとき、ステップS304~S318が繰返される。この場合は、RAM1103に格納されたデータベース(1)の全てのコンテンツID(1)~コンテンツID( $N(m)$ )と検索結果データベースのコンテンツID(1)~コンテンツID(S)とが一致するか否かの判定が行なわれる。

【0159】そして、ステップS318において $n=N(m)$ であると判定されたとき、 $m=m+1$ に設定され(ステップS320)、コントローラ1106は、 $m=M$ であるか否かを判定する(ステップS322)。ここで、 $M$ は、RAM1103に格納されたデータベースの総数を表す。ステップS322において $m=M$ でないと判定されたとき、ステップS302~S322が繰返される。すなわち、RAM1103に格納されたM個のデータベースに検索結果データベースのコンテンツID(1)~コンテンツID(S)が含まれるか否かが判定される。そして、ステップS322において、 $m=M$ であると判定されたとき、データベースの検索動作が終了

する(ステップS324)。その結果、図19に示す検索結果データベースの所有端末ID1, 2, ...の欄、およびライセンス有無の欄にデータが格納される。そして、コントローラ1106は、各コンテンツIDを含むデータベースを保持する端末IDの個数を所有端末数の欄に格納する。図19においては、コンテンツID(6)に対応する所有端末数が「2」になっているが、これは、コンテンツID(6)を含むデータベースが2つの端末に保持されていることを示す。なお、所有端末ID1, 2, ...は、コンテンツID(1)〜コンテンツID(S)を含むデータベースが保持されている端末が判明した順序を示す。したがって、1番目に判定した端末IDは所有端末ID1の欄に格納される。以下、同様にして2番目、3番目、...に判定した端末IDが所有端末ID2, ID3, ...の欄に格納される。

【0160】このように、携帯電話機100のコントローラ1106は、配信サーバ10から検索結果を受信したとき、検索結果データベースを作成する。そして、コントローラ1106は、作成した検索結果データベースからタイトル名、所有端末ID、およびライセンス有無を抽出し、タイトル名、所有端末IDから判明する所有者、およびライセンスの有無を表示パネル1110に画面177(図13参照)として表示する。

【0161】また、図13の画面178, 179および図14の画面180~182によって表される携帯電話機101, 102からの暗号化コンテンツデータのコピー(複製)は、図20に示すフローチャートに従って行なわれる。携帯電話機101, 102に装着されたメモリカード111, 112から携帯電話機100に装着されたメモリカード110へ暗号化コンテンツデータをコピーする場合、携帯電話機101, 102のコントローラ1106と携帯電話機100のコントローラ1106とがデータの授受に関与するが、図20においては、説明の便宜上、1つのコントローラを示し、その1つのコントローラは、携帯電話機101, 102のコントローラ1106の機能と携帯電話機100のコントローラ1106の機能とを果たすこととしている。また、図20に示す処理に入る前に、送信側である携帯電話機101, 102のユーザは、メモリカード111, 112を携帯電話機101, 102に装着し、携帯電話機100のユーザからの暗号化コンテンツデータのコピー要求に対して許可を与えているものとする。

【0162】図20を参照して、複製リクエストがユーザから指示されると(ステップS400)、携帯電話機100のコントローラ1106は、メモリカード110へ認証データの送信要求をメモリカードインタフェース1200を介してメモリカード110へ送信する(ステップS402)。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して認証データの送信要求を

受信する(ステップS404)。

【0163】メモリカード110のコントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{K P m 3 / / C m 3} K P aをバスBS3を介して読出し、その読出した認証データ{K P m 3 / / C m 3} K P aをバスBS3、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ出力する(ステップS406)。そして、携帯電話機100のコントローラ1106は、メモリカードインタフェース1200を介して認証データ{K P m 3 / / C m 3} K P aを受取り、送受信部1102およびアンテナ1101を介して携帯電話機101, 102へメモリカード110の認証データ{K P m 3 / / C m 3} K P aを送信する(ステップS408)。

【0164】そうすると、携帯電話機101, 102のコントローラ1106は、アンテナ1101および送受信部1102を介して認証データ{K P m 3 / / C m 3} K P aを受信し、バスBS2およびメモリカードインタフェース1200を介してメモリカード111, 112へ認証データ{K P m 3 / / C m 3} K P aを入力する(ステップS408)。メモリカード111, 112のコントローラ1420は、端子1426およびインタフェース1424を介して認証データ{K P m 3 / / C m 3} K P aを受信し、その受信した認証データ{K P m 3 / / C m 3} K P aをバスBS3を介して復号処理部1408へ与える。そして、復号処理部1408は、K P a保持部1414からの認証鍵K P aによって認証データ{K P m 3 / / C m 3} K P aの復号処理を実行する(ステップS410)。コントローラ1420は、復号処理部1408における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードであって、メモリカード110から正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS412)。正当な認証データであると判断された場合、コントローラ1420は、認証データから取得されたクラス公開暗号鍵K P m 3およびクラス証明書C m 3を承認し、受理する。そして、次の処理(ステップS414)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を受理しないで処理を終了する(ステップS420)。

【0165】認証の結果、正当な認証データを持つメモリカードへの暗号化コンテンツデータの複製であることが確認されると、メモリカード111, 112において、コントローラ1420は、バスBS3を介してメモリ1415のデータ領域1415Cから暗号化コンテンツデータ{D c} K cおよび付加情報D c - i n fを読出し、バスBS3、インタフェース1424および端子

10

20

30

40

50

1426を介して{Dc}Kc//Dc-infを出力する(ステップS414)。携帯電話機101、102のコントローラ1106は、メモリカードインタフェース1200およびバスBS2を介して{Dc}Kc//Dc-infを受信し、送受信部1102およびアンテナ1101を介して{Dc}Kc//Dc-infを携帯電話機100へ送信する(ステップS416)。

【0166】携帯電話機100のコントローラ1106は、アンテナ1101および送受信部1102を介して{Dc}Kc//Dc-infを受信し、バスBS2およびメモリカードインタフェース1200を介して{Dc}Kc//Dc-infをメモリカード110へ入力し、メモリカード110のコントローラ1420は、端子1426およびインタフェース1424を介して{Dc}Kc//Dc-infを受取る。そして、コントローラ1420は、バスBS3を介して{Dc}Kc//Dc-infをメモリ1415のデータ領域1415Cに格納して(ステップS418)、暗号化コンテンツデータの複製動作が終了する(ステップS420)。

【0167】携帯電話機100のユーザは、暗号化コンテンツデータの複製が終了した後、図7および図8に示したフローチャートに従って、複製した暗号化コンテンツデータを復号および再生するためのライセンスの配信要求を配信サーバ10へ送信し、配信サーバ10からライセンスを受信してメモリカード110に格納する。

【0168】このように、携帯電話機100のユーザは、新たに購入したい曲が携帯電話機101、102に装着されるメモリカード111、112に格納されていることを確認すると、携帯電話機101、102から暗号化コンテンツデータを複製し、その複製した暗号化コンテンツデータのライセンスを配信サーバ10から受信する。

【0169】この発明の実施の形態によれば、携帯電話機のユーザは、新たに購入したい曲がどこに格納されているかを検索した後、暗号化コンテンツデータが格納されているメモリカードから暗号化コンテンツデータを複製するので、購入したい曲の受信に長時間を必要とせず、そのための通信費を節約できる。

【0170】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0171】

【発明の効果】本発明によれば、携帯電話機のユーザは、新たに購入したい曲がどこに格納されているかを検索した後、暗号化コンテンツデータが格納されているメモリカードから暗号化コンテンツデータを複製するので、購入したい曲の受信に長時間を必要とせず、そのた

めの通信費を節約できる。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図5】 図1に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図6】 図1に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図7】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図8】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図9】 メモリカードにおける再生リストファイルの構成を示す図である。

【図10】 図9に示すコンテンツファイルに記録された暗号化コンテンツデータと付加情報との関係を示す概念図である。

【図11】 携帯電話機における再生動作を説明するためのフローチャートである。

【図12】 暗号化コンテンツデータを管理するためのデータベースの概念図である。

【図13】 携帯電話機における各動作時に表示パネルに示される画面を示す図である。

【図14】 携帯電話機における各動作時に表示パネルに示される画面を示す図である。

【図15】 複数のデータベースを管理するための一覧表の概念図である。

【図16】 購入したい曲の配信サーバにおける検索動作を説明するためのフローチャートである。

【図17】 配信サーバから受信した検索結果に含まれる暗号化コンテンツデータの携帯電話機における検索動作を説明するためのフローチャートである。

【図18】 配信サーバから送信される検索結果の例である。

【図19】 携帯電話機における検索結果を示すデータベースの概念図である。

【図20】 他の携帯電話機からの暗号化コンテンツデータの複製動作を説明するためのフローチャートである。

【符号の説明】

10 配信サーバ、20 配信キャリア、65 専用ケーブル、100~102 携帯電話機、110~112 メモリカード、130~132 ヘッドホン、150 データベース、155 一覧表、160 再生リス

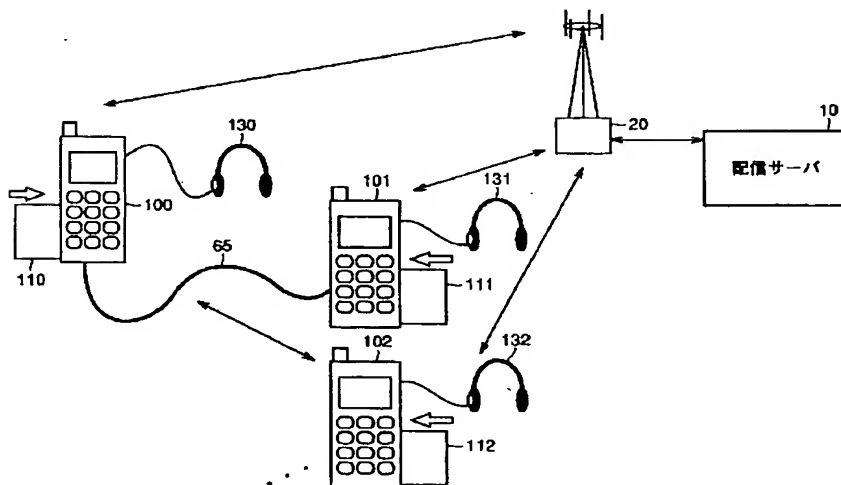
35

トファイル、163 コンテンツ管理情報、165 エントリ管理情報、166 カードID、170~184

画面、302 課金データベース、304 情報データベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1404、1408、1412、1422、1504、1510、1516 復号処理部、313 認証鍵保持部、315 配信制御部、316、1418、1508 セッションキー発生部、318、326、328、1406、1410、1417、1506 暗号処理部、350 通信装置、1101 アンテナ、1102 送受信部、1103 RAM、1106、1420 コントローラ、1112 USBインタフェース、1114、1426、1530 端子、1108 キー操作部、1110 表示パネル、1200 メモリカードインタフェース、1400、1500 認証データ保\*

\*持部、1402 Kmc保持部、1414 KPa保持部、1415 メモリ、1415A ログ領域、1415B ライセンス領域、1415C データ領域、1416 KPmc保持部、1421 Km保持部、1424 インタフェース、1442、1446 切換スイッチ、1502 Kpl保持部、1518 音楽再生部、1519 DA変換器、1531 コンテンツNo、1532 コンテンツID、1533 タイトル名、1534 アーティスト名、1535 コンテンツ種別、1536 ライセンス有無、1537 格納カードID、1550コンテンツ再生デバイス、1551 データベースNo、1552 データベース、1553 コンテンツ数、1554 端末ID、1555 所有者名、1621~162n ライセンス管理ファイル、1611~161n コンテンツファイル、1631~1640 コンテンツデータ、1651~1660 管理情報。

【図1】

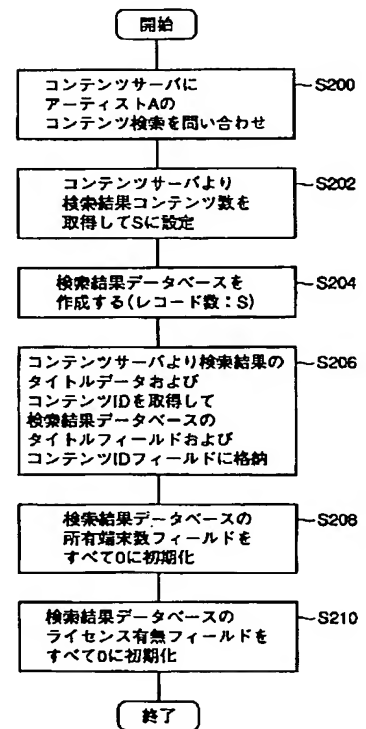


【図2】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ (Dc)Kcとして配信され、メモリカードに保持される
Dc-Inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+コンテンツID+ライセンスIDの総称
有効フラグ	フラグ	ライセンス固有	ライセンスをメモリカードから外部へ出すことが可能か否かを表す。

36

【図16】



【図18】

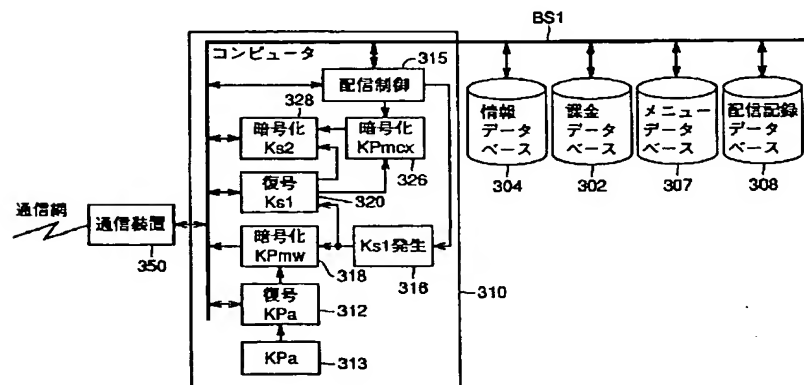
No	コンテンツID	タイトル名
1	878172	タイトル1
2	231243	タイトル2
3	434345	タイトル3
4	344567	タイトル4
5	324325	タイトル5
6	434255	タイトル6
...	...	...
S	322432	タイトルS

【図3】

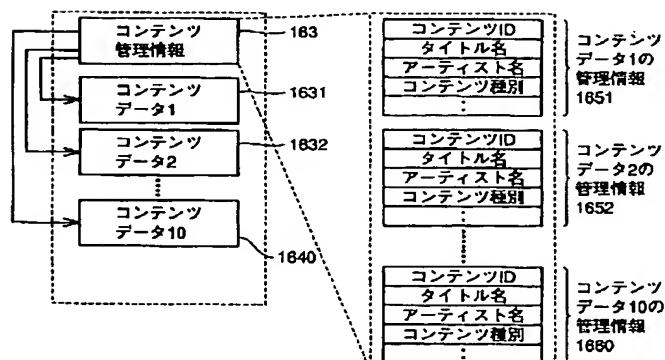
	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム共有	認証局にて認証データを復号する鍵
	Ks1	共通鍵	セッション固有	メモリカードへのライセンス配信ごとに発生
メモリカード	KPa	公開認証鍵	システム共有	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカードのクラス証明書。 認証機能を有する。 (KPmw/Cmw)KPaの形式で出荷時に記録。 *メモリカードのクラスごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cpyとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 (KPpy/Cpy)KPaの形式で出荷時に記録。 *コンテンツ再生デバイスのクラスyごとに異なる。

【図4】

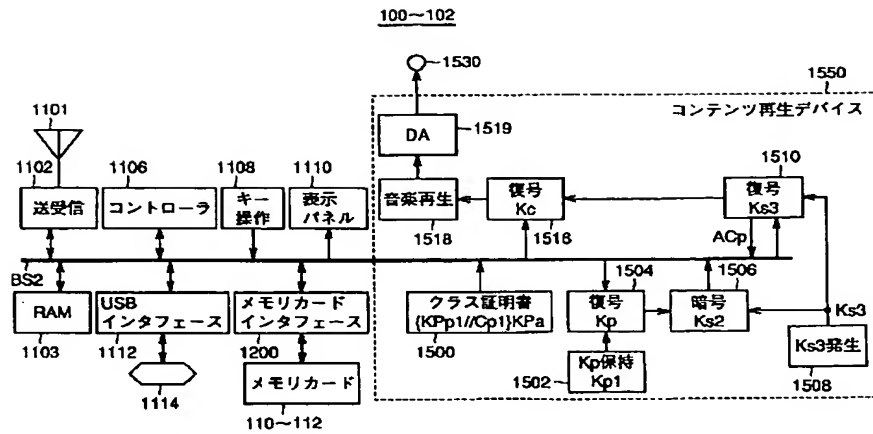
10



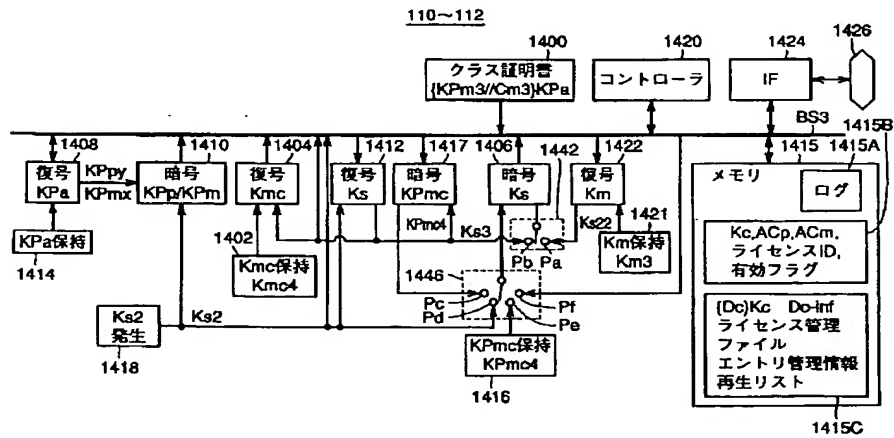
【図10】



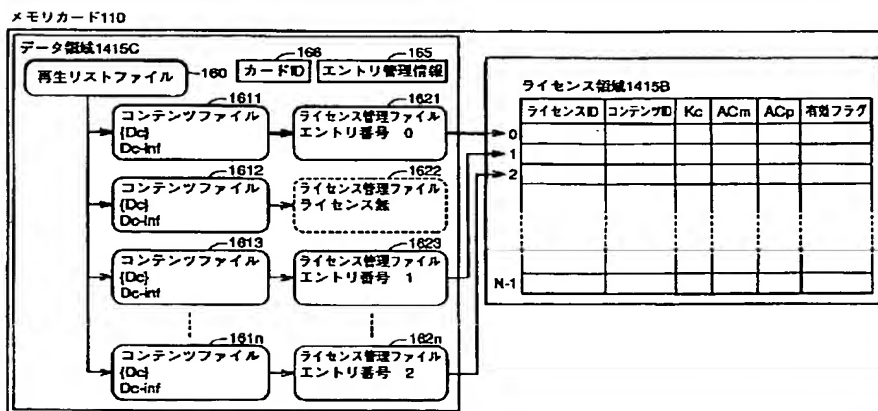
【図5】



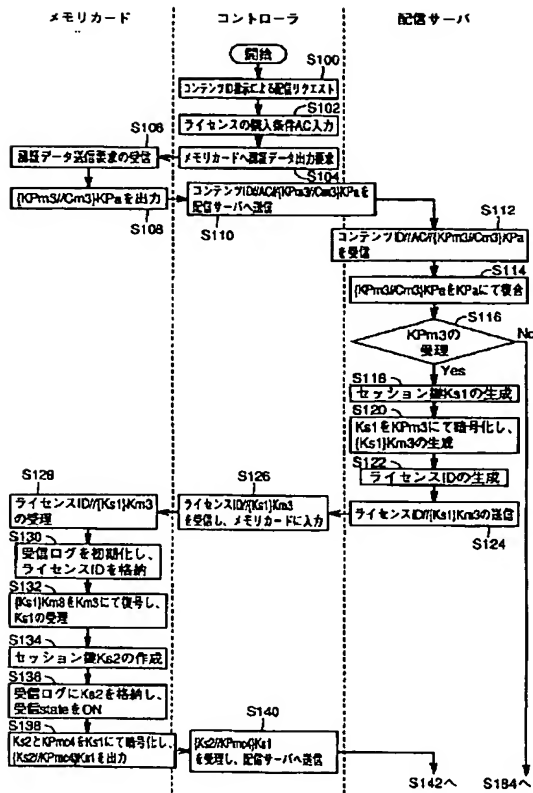
【図6】



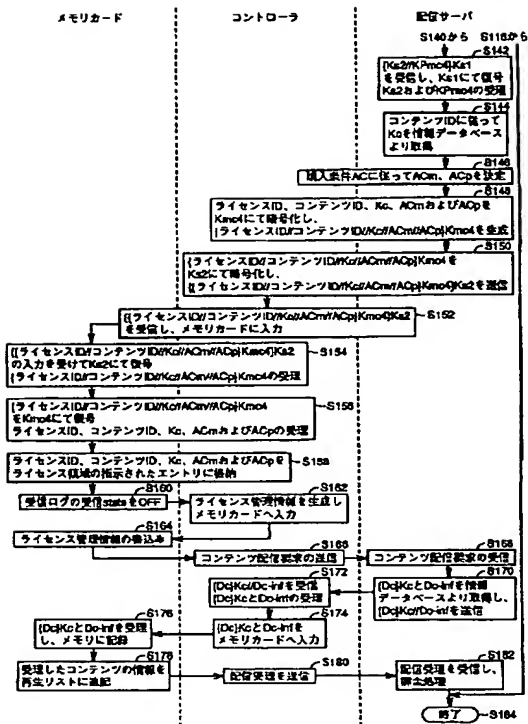
【図9】



【図7】



【図8】



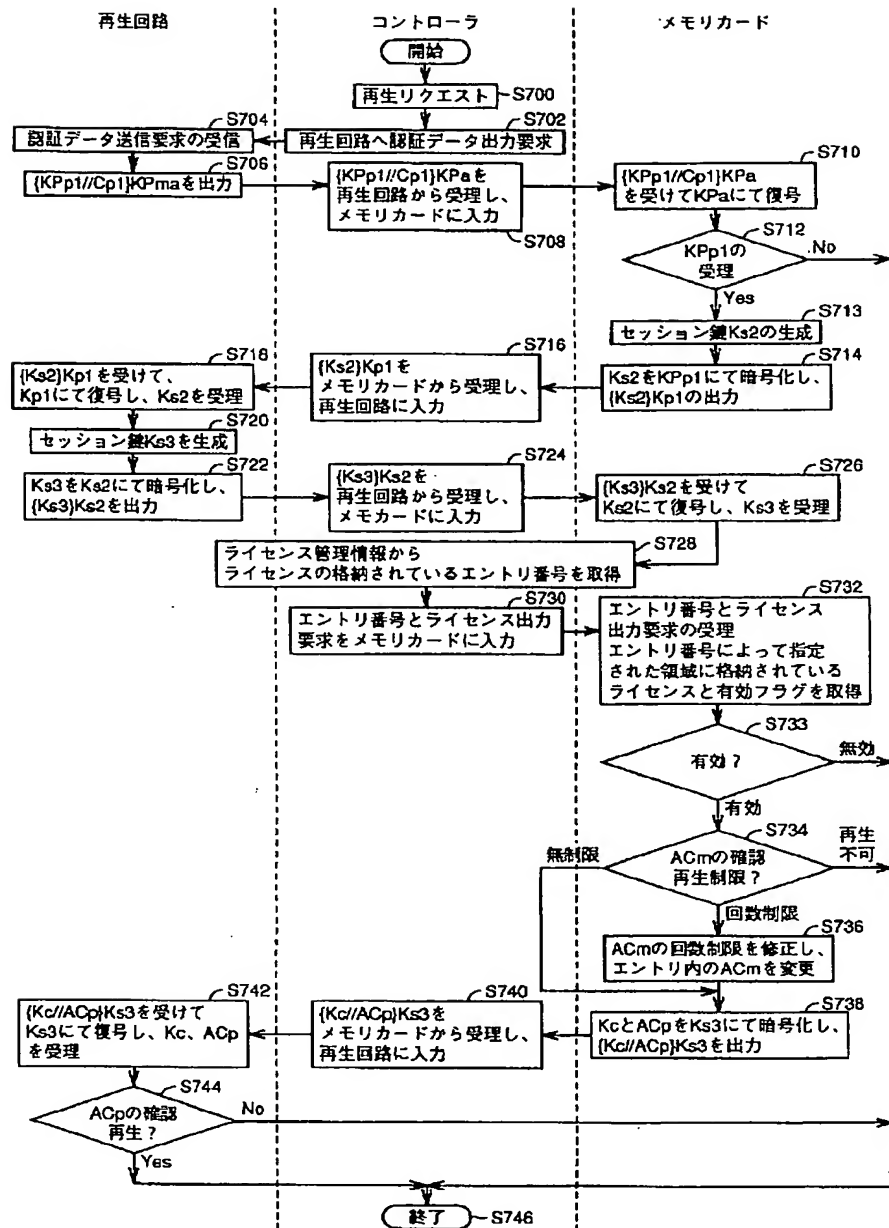
【図12】

	1531	1532	1533	1534	1535	1536	1537
	コンテンツNo	コンテンツID	タイトル名	アーティスト名	コンテンツ種別	ライセンス有無	格納カードID
150	1	CONTID(1)	タイトル1	アーティスト1	ロック	1	CARDID(1)
	2	CONTID(2)	タイトル2	アーティスト2	クラシック	1	CARDID(2)
	3	CONTID(3)	タイトル3	アーティスト3	英会話	0	CARDID(3)
	⋮	⋮	⋮	⋮	⋮	⋮	⋮
	N	CONTID(N)	タイトルN	アーティストN	ニュース	1	CARDID(4)

【図15】

	1551	1552	1553	1554	1555
	データベースNo	コンテンツデータベース	コンテンツ数	端末ID	所有者名
155	1	コンテンツデータベース(1)	N(1)	端末ID(1)	OWNER(1)
	2	コンテンツデータベース(2)	N(2)	端末ID(2)	OWNER(2)
	3	コンテンツデータベース(3)	N(3)	端末ID(3)	OWNER(3)
	⋮	⋮	⋮	⋮	⋮
	M	コンテンツデータベース(M)	N(M)	端末ID(M)	OWNER(M)

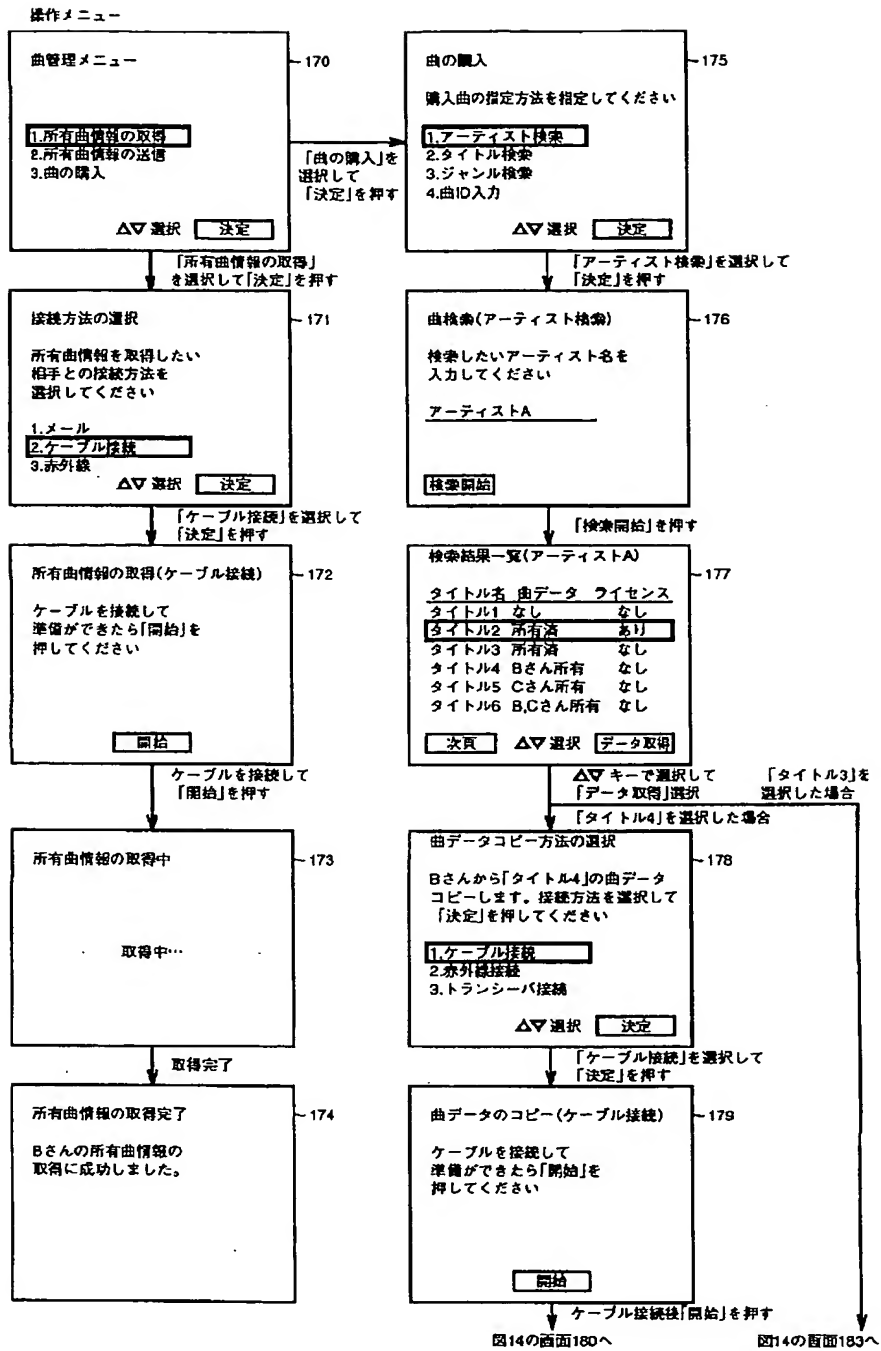
【図11】



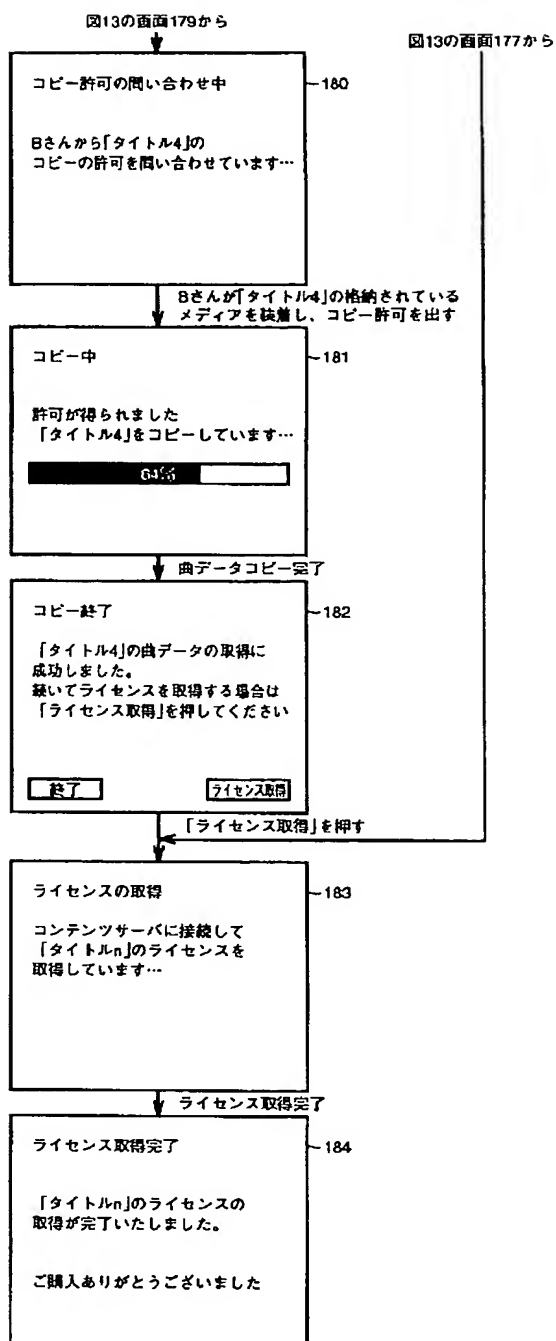
【図19】

検索番号	コンテンツID	タイトル名	所有端末数	所有端末ID1	所有端末ID2	.....	ライセンス有無
1	CONTID(1)	タイトル(1)	0	0	0		0
2	CONTID(2)	タイトル(2)	1	端末ID1(2)	0		1
3	CONTID(3)	タイトル(3)	1	端末ID1(3)	0		0
4	CONTID(4)	タイトル(4)	1	端末ID1(4)	0		0
5	CONTID(5)	タイトル(5)	1	端末ID1(5)	0		0
6	CONTID(6)	タイトル(6)	2	端末ID1(6)	端末ID2(6)		0
⋮	⋮	⋮	⋮	⋮	⋮		⋮
S	CONTID(S)	タイトル(S)	0	0	0		0

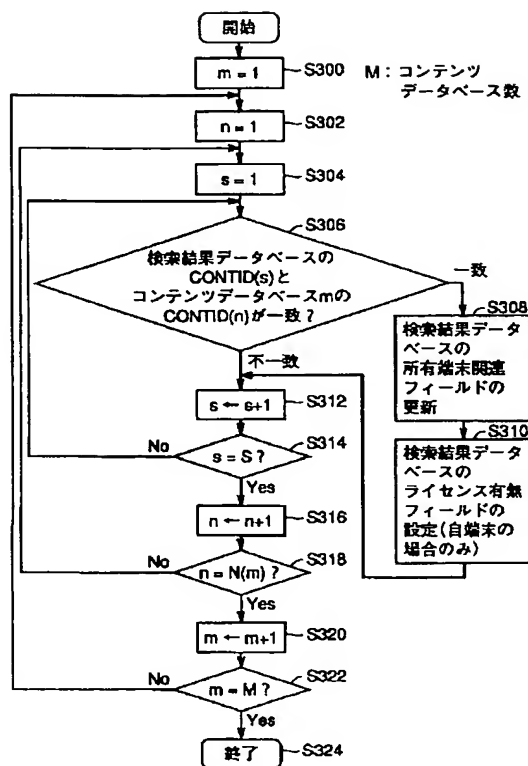
【図13】



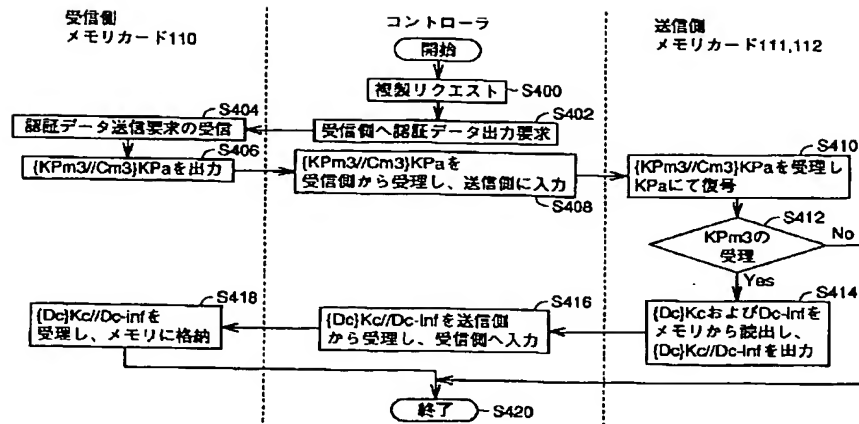
【図14】



【図17】



【図20】



フロントページの続き

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E
17/30	1 1 0	17/30	1 1 0 F
	1 7 0		1 7 0 Z
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 S
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B

F ターム (参考)

5B017 AA06 BA09 CA16  
 5B075 ND16 PP23 PQ02  
 5B082 HA05  
 5J104 AA01 AA16 EA01 EA04 EA16  
 NA03 PA02 PA07  
 5K067 AA32 BB04 DD17 EE02 EE10  
 EE16 FF02 FF23 GG01 GG11  
 HH05 HH22 HH23 HH36

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**